

---

# Enodia Bridge

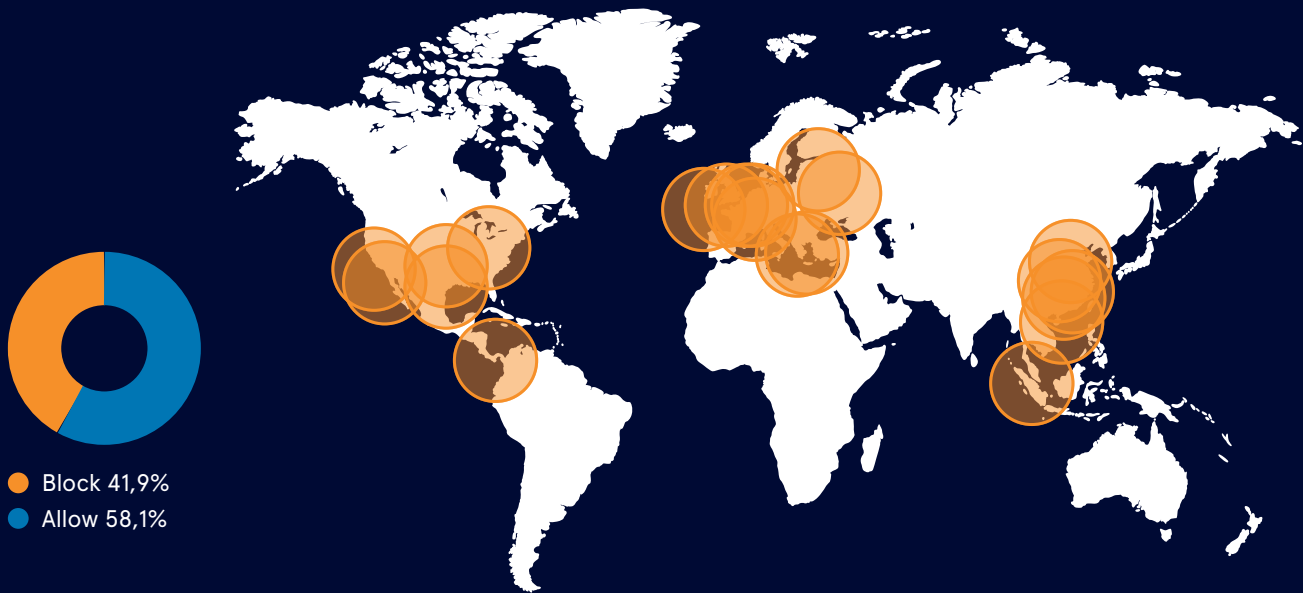
- Additional hardening of your public facing networks with dynamic Block lists on the L2/L3 layer.
- Additional DNS protection with dynamic Allow and Block lists.
- Encrypted DNS (DoH, DoT & DoQ).
- Optional DNSSEC end-to-end.
- Can run on your own hardware.





## Free 30 days scoring of your traffic on our collector in the cloud. You can see how much we would filter on your specific traffic. Requires that your NAT firewall can send Meta Data to our destination. I.e. syslog.

Also possible to identify traffic leaving your networks towards our IOCs)



- Harvesting IOCs from our own honeypots in Europe.
- Collection from more than 100 dynamic and curated lists.
- Around 1 million lines in our signature IP Block List. Updated every 10th minute.
- More than 10 million FQDNs in our DNS firewall. Updated every hour.
- Avoid scanners and "Drive-By" hackers. We estimate that more than 90% of known IOCs and their infrastructure are already on our lists.
- Additional DNS Block lists like Crypto, Adult & Gambling (and more) available.
- Washing against known "good" sources and destinations to avoid false positives.
- In a hosting context, we see between 30% - 60% of ingress traffic is actually unwanted.
- All logging can be sent to your own syslog/SIEM. Both the IP and DNS firewall logs.
- Optional High Availability with two devices.